AMENDMENT AND PRESENTATION OF CLAIMS

Please replace all prior claims in the present application with the following claims, in which claims 1 and 13-17 are currently amended.

1. (Currently Amended) A method for authenticating transmitted data in real time, said data transmitted as a stream of packets over a publicly available medium, the method comprising the steps of:

(a) generating a master cryptographic key pair, including a first public key and a first private key;

(b) publishing a first certificate issued by a certificate authority, the first certificate including the first public key and a first digital signature of the first public key based on a private key from the certificate authority;

(c) generating a disposable cryptographic key pair, including a second public key and second private key;

(d) generating a second certificate, the second certificate including the second public key and a second digital signature of the second public key based on the first private key;

(e) publishing the second certificate;

(f) signing the packets of data to be transmitted with a third digital signature by processing the data to be transmitted through a first one way hashing function to generate a first hash value and encrypting the first hash value utilizing the second private key;

(g) processing received data through the first one way hashing function to create a second hash value;

(h) decrypting the received third digital signature utilizing the second public key to obtain a third hash value; and

(i) verifying authenticity of the received data by comparing the second hash value to the third hash value,

wherein the first private key, the second private key, and the private key from the certificate authority have different values.

2. (Original) The method for authenticating transmitted data in real time according to claim 1, wherein the step of generating a master key pair comprises creating long first public and private keys.

3. (Previously Presented) The method for authenticating transmitted data in real time according to claim 1, wherein the first certificate further includes an identification of a sender and an identification of a certificate authority issuing the first certificate.

4. (Previously Presented) The method for authenticating transmitted data in real time according to claim 3, wherein the first digital signature is produced by:

(a) processing information representing the identification of the sender, the identification of the certificate authority issuing the first certificate and the first public key through a second one way hashing function to create a fourth hash value; and

(b) encrypting the fourth hash value utilizing the private key from the certificate authority issuing the first certificate to create the first digital signature.

5. (Previously Presented) The method for authenticating transmitted data in real time according to claim 4, further comprising the step of verifying authenticity of data comprising the first certificate.

6. (Previously Presented) The method for authenticating transmitted data in real time according to claim 5, wherein the step of verifying the authenticity of the data comprising the first certificate comprises:

(a) decrypting the first digital signature to obtain a fifth hash value utilizing a public key issued by the certificate authority issuing the first certificate;

(b) processing the received information representing the identification of the sender, the identification of the certificate authority issuing the first certificate and the first public key through the second one way hashing function to create a sixth hash value; and

(c) comparing the fifth and sixth hash values.

7. (Original) The method for authenticating transmitted data in real time according to claim 1, wherein the step of generating a disposable cryptographic key pair comprises generating short second public and private keys.

8. (Previously Presented) The method for authenticating transmitted data in real time according to claim 1, wherein the second certificate further includes the identification of the sender and an identification of a signing authority issuing the second certificate.

9. (Previously Presented) The method for authenticating transmitted data in real time according to claim 8, wherein the second digital signature is produced by:

(a) processing the data representing the identification of the sender, the identification of the signing authority issuing the second certificate and the second public key through a third one way hashing function to create a seventh hash value; and

(b) encrypting the seventh hash value utilizing the first private key to create the second digital signature.

10. (Previously Presented) The method for authenticating transmitted data in real time according to claim 9, further comprising the step of verifying the authenticity of the data comprising the second certificate.

11. (Previously Presented) The method for authenticating transmitted data in real time according to claim 10, wherein the step of verifying the authenticity of the data comprising the second certificate comprises:

(a) decrypting the second digital signature to obtain an eighth hash value utilizing the first public key;

(b) processing the received data representing the identification of the sender, the identification of the signing authority issuing the second certificate and the second public key through the third one way hashing function to create a ninth hash value; and

(c) comparing the eighth and ninth hash values.

12. (Previously Presented) The method for authenticating transmitted data in real time according to claim 1, further comprising dividing the data into packets and signing and authenticating each packet of data in accordance with steps (f) through (i) of claim 1.

13. (Currently Amended) A method for digitally signing data in real time, <u>said data to be transmitted as a stream of packets over a publicly available medium,</u> the method comprising the steps of:

(a) generating a master key pair including a first public key and a first private key;

(b) publishing a first certificate, the first certificate including the first public key and a first digital signature based on a key pair of a certificate authority;

(c) generating a disposable key pair, the disposable key pair including a second public key and a second private key, and wherein the disposable key pair is shorter than the master key pair;

(d) generating a second certificate, the second certificate including the second public key and a second digital signature based on the master key pair;

(e) dividing the data to be signed into the packets;

(f) for each packet of data, computing a hash value based on the data in the packet utilizing a one way hashing function;

(g) encrypting the hash value utilizing the second private key as the encryption key; and

(h) coupling each encrypted hash value with its corresponding data packet.

14. (Currently Amended) A method for verifying digitally signed data in real time, said data transmitted as a stream of packets over a publicly available medium, the method comprising the steps of:

(a) processing a data portion of the digitally signed data through a one way hashing function to obtain a first hash value for each of the packets of digitally signed data;

(b) verifying contents of a first certificate issued by a certificate authority utilizing a public key issued by the certificate authority, the first certificate including a first public key of a long master key pair;

(c) verifying contents of a second certificate issued by a sender of the data utilizing the first public key from the first certificate, the second certificate including a second public key of a short disposable key pair that is shorter than the long master key pair;

(d) decrypting a digital signature portion of the digitally signed data utilizing the second public key to obtain a second hash value; and

(e) comparing the first and second hash values.

15. (Currently Amended) A method for digitally signing data in real time, said data to be transmitted as a stream of packets over a publicly available medium, the method comprising the steps of:

(a) generating a disposable key pair, the disposable key pair including a short public key and a short private key;

(b) publishing the short public key and a digital signature of the short public key based on a long private key longer than the short private key;

(c) dividing data to be signed into the packets;

(d) for each packet of data, computing a hash value based on the data in the data packet utilizing a one way hashing function;

(e) encrypting the hash value utilizing the short private key; and

(f) coupling each encrypted hash value with its corresponding data packet.

16. (Currently Amended) A method for verifying digitally signed data in real time, said data transmitted as a stream of packets over a publicly available medium, the method comprising the steps of:

(a) processing a data portion of the digitally signed data through a one way hashing function to obtain a first hash value for each of the packets of digitally signed data;

(b) decrypting a digital signature portion of the digitally signed data utilizing a published short public key to obtain a second hash value;

(c) comparing the first and second hash values; and

(d) verifying a digital signature of the short public key based on a long public key, wherein the short public key is shorter than the long public key.

17. (Currently Amended) A method for verifying digitally signed data in real time, said data transmitted as a stream of packets over a publicly available medium, the method comprising the steps of:

receiving ~~a data~~ one of the packets including an unencrypted data portion and a digital signature portion;

generating a first hash value by processing the received unencrypted data portion through a one way hashing function;

decrypting the received digital signature utilizing a first public key to obtain a second hash value;

verifying the digitally signed data by comparing the first hash value to the second hash value; and

verifying the first public key based on a digital signature of a second public key issued by a certificate authority and having a different value than the first public key.